****

**Media alert**

**Sophos onthult aanvalstechnieken van de meest voorkomende ransomwarefamilies**

* *Playbook voor verdedigers omvat aanvalstools en -technieken die worden gebruikt door elf grote ransomware-families waaronder WannaCry, SamSam, RobbinHood, Ryuk, MegaCortex*
* *Automated, Active Attack meest voorkomende aanpak onder de beste ransomwarefamilies in rapport*

**OOSTERHOUT, NL** – 19 nov. 2019 - Sophos lanceert [How Ransomware Attacks](https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf), een playbook waarin wordt uitgelegd hoe ransomwarevarianten aanvallen. Het is een aanvulling op het 2020 Threat Report dat begin november is uitgebracht en bevat een gedetailleerde analyse van elf van de meest voorkomende en hardnekkige ransomwarefamilies.

Het SophosLabs-onderzoek benadrukt hoe ransomware onopgemerkt beveiligingscontroles tracht te omzeilen door vertrouwde processen te misbruiken, en vervolgens interne systemen gebruikt om zoveel mogelijk bestanden te versleutelen en back-up- en herstelprocessen uit te schakelen voordat een IT-beveiligingsteam de schade kan herstellen.

De tools en technieken die onder het *playbook* vallen, zijn onder meer:

**De voornaamste distributiemethoden voor de belangrijkste ransomwarefamilies**. Ransomware wordt meestal op een van de volgende manieren gedistribueerd: als *cryptoworm* die zichzelf snel kopieert naar andere computers voor maximale impact (WannaCry), als *ransomware-as-a-service* verkocht op het dark web als distributiekit (Sodinokibi) of door middel van een *Automated Active Adversary*-aanval, waarbij aanvallers ransomware handmatig inzetten na een geautomatiseerde netwerkscan voor systemen met een zwakke bescherming. Deze automated, active attack-stijl was een van de meest voorkomende benaderingen door topfamilies in het rapport.

**Cryptographic code signing-ransomware** met een gekocht of gestolen digitaal certificaat om zo beveiligingssoftware te overtuigen dat de code betrouwbaar is en geen analyse nodig heeft.

**Privilege escalation** met behulp van reeds beschikbare exploits, om toegangsrechten te verwerven. Hiermee kan de aanvaller programma's zoals Remote Access Tools installeren en gegevens bekijken, wijzigen of verwijderen, nieuwe accounts met volledige gebruikersrechten maken en beveiligingssoftware uitschakelen.

**Laterale verplaatsing** en zoeken in het netwerk naar bestands- en back-upservers en hierbij onder de radar blijven om de volledige impact van een ransomware-aanval te ontketenen. Binnen een uur kunnen aanvallers een script maken om de ransomware te kopiëren en op endpoints en servers los te laten. Om de aanval te versnellen, kan de ransomware voorrang geven aan data op externe/gedeelde schijven, zich eerst richten op kleinere documentgroottes en tegelijkertijd meerdere versleutelingsprocessen uitvoeren.

**Externe aanvallen**. File servers worden zelf vaak niet besmet met ransomware. In plaats daarvan wordt de dreiging meestal uitgevoerd op een of meer endpoints, waarbij een gebruikersaccount wordt misbruikt om documenten op afstand aan te vallen, soms via het Remote Desktop Protocol of gericht op remote monitoring and management (RMM) die doorgaans worden gebruikt door MSP’s om de IT-infrastructuur en/of eindgebruikerssystemen van klanten te beheren.

**Bestandsversleuteling en hernoemen**. Er is een aantal methoden voor bestandsversleuteling, waaronder het overschrijven van documenten, maar de meeste gaan gepaard met het verwijderen van de back-up of de originele kopie om zo het herstelproces te belemmeren.

Het playbook legt uit hoe deze en andere tools en technieken worden geïmplementeerd door de volgende elf ransomwarefamilies: WannaCry, GandCrab, SamSam, Dharma, BitPaymer, Ryuk, LockerGoga, MegaCortex, RobbinHood, Matrix en Sodinokibi.

Sophos’ Mark Loman, auteur van het rapport: “Ransomwarebedenkers begrijpen goed hoe beveiligingssoftware werkt en passen hierop hun aanvallen aan. Alles is ontworpen om detectie te voorkomen, terwijl de malware zoveel mogelijk documenten zo snel mogelijk versleutelt. Daarbij proberen ze het slachtoffers zo moeilijk, zo niet onmogelijk te maken de gegevens te herstellen. In sommige gevallen vindt het grootste deel van de aanval 's nachts plaats. Tegen de tijd dat het slachtoffer ziet wat er aan de hand is, is het te laat. Het is van vitaal belang over robuuste beveiligingscontroles, monitoring en respons te beschikken die alle endpoints, netwerken en systemen dekken. Daarna is het minstens zo belangrijk software-updates te installeren wanneer deze worden uitgegeven.”

**Over Sophos**

Als wereldwijde leider in *next-gen* cybersecurity beschermt Sophos meer dan 400.000 organisaties in meer dan 150 landen tegen de meest geavanceerde cyberdreigingen. Aangedreven door SophosLabs, een wereldwijd team voor *threat intelligence* en *data science*, beschermen de cloudgebaseerde en AI-aangedreven oplossingen laptops, servers, mobiele devices en netwerken tegen immer evoluerende cyberaanvaltechnieken waaronder ransomware, malware, exploits en phishing.

Het cloudgebaseerde beheerplatform Sophos Central integreert het volledige portfolio van Sophos’ *next-gen* oplossingen (waaronder de endpointoplossing Intercept X en XG next-gen firewall) in een enkel ‘gesynchroniseerd beveiligingssysteem’ dat via een set API's toegankelijk is. Sophos verkoopt zijn oplossingen en diensten via een wereldwijd kanaal van meer dan 47.000 partners en Managed Service Providers. Sophos stelt zijn innovatieve commerciële technologieën via Sophos Home ook beschikbaar aan consumenten. Het bedrijf heeft zijn hoofdkantoor in Oxford (VK) en wordt op de London Stock Exchange onder het symbool *‘SOPH’* verhandeld. Voor meer informatie: [www.sophos.com](http://www.sophos.com).

**Voor meer informatie, interviewmogelijkheden of beeldmateriaal:**

Square Egg Communications, Sandra Van Hauwaert, [sandra@square-egg.be](mailto:sandra@square-egg.be), GSM 0497251816.